Devoir de Mathématiques n°2

Kévin Polisano
MP*

Jeudi 17 septembre 2009

Première partie

1. a) $J(\alpha)$ non vide car α algébrique. Sg additif car $\forall (P,Q) \in J(\alpha)^2 \Rightarrow (P-Q)(\alpha) = 0$.

$$\forall (P,Q) \in K[X] \times J(\alpha), (PQ)(\alpha) = P(\alpha)Q(\alpha) = 0 = Q(\alpha)P(\alpha) = (QP)(\alpha) \text{ car } Q(\alpha) = 0$$

$J(\alpha)$ est un idéal. $K[X]$ est principal donc ses idéaux sont principaux : $J(\alpha) = M_\alpha K[X]$.

M_α est forcément de degré minimal parmi les polynômes de $J(\alpha)$. On peut le choisir unitaire quitte à diviser par le coefficient dominant. Il est unique car s'il en existait un autre ils se diviseraient mutuellement et étant unitaires ils sont égaux. Irréductible car si $M_\alpha = PQ$ alors $M_\alpha(\alpha) = 0 = P(\alpha)Q(\alpha)$, par intégrité l'un des facteurs est nul, absurde par minimalité de M_α.

b) Le sens direct est trivial car $M_\alpha(\alpha) = 0$. Pour l'autre sens :

$$P(\alpha) = 0 \Rightarrow P \in J(\alpha) \Rightarrow P = QM_\alpha \Rightarrow Q = 1 \text{ car } P \text{ irréductible}$$

2) $i/ \Rightarrow ii/$: $\alpha \in K$, $P(X) = X - \alpha = M_\alpha(X)$ convient. Réciproquement si $M_\alpha(X) = X - k$ avec $k \in K$ alors $\alpha = k \in K$. $i/ \Rightarrow iii/$: $\alpha \in K[\alpha] = K$. $i/ \Rightarrow iii/$: $\alpha \in K$ donc $K[\alpha] \subset K$, et $x \in K$ s'écrit $x = 1.x \in K[\alpha]$ d'où $K = K[\alpha]$.

3. a) $M_\alpha(X) = X^2 + aX + b$ d'où $\alpha^2 = -a\alpha - b \Rightarrow (1, \alpha)$ génératrice de $K[\alpha]$.

Libre car $x_0 + x_1\alpha = 0 \Rightarrow x_0 = x_1 = 0$ par minimalité de M_α.

Tout élément de $K[\alpha]$ s'écrit donc $x = x_0 + x_1\alpha = R(\alpha)$, $\deg(R) = 1$.

Comme M_α est irréductible, ils sont premiers entre eux donc il existe U, V tq :

$VM_\alpha + UR = 1$, et en évaluant en α : $U(\alpha)R(\alpha) = 1 \Rightarrow x$ inversible.

b) $\alpha^2 + a\alpha + b = 0$ donc α est une des racines : $\dfrac{-a \pm \sqrt{a^2 - 4b}}{2}$.

Posons $k = a^2 - 4b$, $x_0 = a$ et $x_1 = 2$. Comme K est un corps $k, x_0, x_1 \in K$ et alors :

$$\alpha = \frac{\sqrt{k} - x_0}{x_1} \Longleftrightarrow \sqrt{k} = x_0 + x_1\alpha$$

Ainsi $\sqrt{k} \in K[\alpha]$ et $K \subset K[\alpha]$ donc $K[\sqrt{k}] \subset K[\alpha]$.

Réciproquement on a $\alpha \in K[\sqrt{k}]$ et $K \in K[\sqrt{k}]$ d'où $K[\alpha] \subset K[\sqrt{k}]$.

On a donc bien trouvé un $k \in K$ tel que $K[\alpha] = K[\sqrt{k}]$.

4. a) $x \in K[\alpha]$, il existe P tel que $x = P(\alpha)$. $P = M_\alpha Q + R$ avec $\deg R < n$.

Donc $x = R(\alpha)$. R unique car si $x = R'(\alpha)$ alors $(R - R')(\alpha) = 0$ absurde car $\deg(R - R') < n$.

Ainsi $(1, \alpha, ..., \alpha^{n-1})$ est une base de $K[\alpha]$ donc $\dim(K[\alpha]) = n$.

b) M_α est irréductible et $\deg(R) < \deg(M_\alpha)$ donc $M_\alpha \wedge R = 1$.

On applique alors le théorème de Bézout : $V(X)M_\alpha(X) + U(X)R(X) = 1 \Rightarrow U(\alpha)R(\alpha) = 1$.

c) L'inverse de $x = R(\alpha)$ est donc $x^{-1} = U(\alpha) \Rightarrow K[\alpha]$ est un corps.

d) $K[\alpha]$ contient α car engendré par cet élément, et K car tout élément de K s'écrit $x = 1.x \in K[\alpha]$. Par ailleurs si un autre corps K' les contient, alors par propriétés des corps (stabilité par $+$ et $\times$) il contient les combinaisons $\sum_{p=0}^{q} x_p \alpha^p$ et donc $K[\alpha]$. En particulier $\mathbb{R}$ contient $K[\alpha]$ car K sous-corps de $\mathbb{R}$.

5. a) Par récurrences directes on trouve $\deg(P_n) = n$, $a_n = 2^n$ et $a_0 = (-1)^n$ (pour $n \geqslant 3$).

$P_2(x) = 4x^2 + 2x - 1$; $P_3(x) = 8x^3 + 4x^2 - 4x - 1$; $P_4(x) = 16x^4 + 8x^3 - 12x^2 - 4x + 1$.

$$Q_{n+2}(x) = P_{n+2}\left(\frac{x}{2}\right) = xP_{n+1}\left(\frac{x}{2}\right) - P_n\left(\frac{x}{2}\right) = xQ_{n+1}(x) - Q_n(x)$$

Initialisation $Q_0(x) = 1$ et $Q_1(x) = x + 1$.

Hérédité : on suppose $Q_n, Q_{n+1} \in \mathbb{Z}[X]$ et par la relation précédente on a bien $Q_{n+2} \in \mathbb{Z}[X]$.

b) $r = \frac{p}{q}, (p, q) \in \mathbb{Z} \times \mathbb{N}$ avec $p \wedge q = 1$. CN : $p | a_0 = (-1)^n$ et $q | a_n = 2^n \times \frac{1}{2^n} = 1$ donc $r = \pm 1$.

$Q_{n+3}(x) + xQ_n(x) = xQ_{n+2}(x) - Q_{n+1}(x) + xQ_n(x) = x(xQ_{n+1}(x) - Q_n(x)) - Q_{n+1}(x) + xQ_n(x)$

$Q_{n+3}(x) + xQ_n(x) = (x^2 - 1)Q_{n+1}(x)$. Ainsi $x = \pm 1$ est racine de Q_{n+3} ssi il est racine de Q_n.

Or $x = \pm 1$ n'est pas racine de Q_0 et Q_2. Seuls les Q_{3k+1} et P_{3k+1} ont des racines rationnelles.

6. a) Eq. caract. : $r^2 - 2\cos(\theta)r + 1 = 0$, discriminant $\Delta = 4(\cos^2(\theta) - 1) = -4\sin^2(\theta) < 0$.

Les racines complexes conjuguées sont donc $e^{\pm i\theta}$ d'où : $u_n = \lambda \cos(n\theta) + \mu \sin(n\theta)$.

Avec $n = 0$ et $n = 1$ on détermine $u_0 = \lambda$ et $\mu = \frac{u_1 - u_0 \cos(\theta)}{\sin(\theta)}$.

b) $P_{n+2}(\cos(\theta)) = 2\cos(\theta)P_{n+1}(\cos(\theta)) - P_n(\cos(\theta)) \Rightarrow v_{n+2} = 2\cos(\theta)v_{n+1} - v_n$.

D'où comme $v_0 = 1$ et $v_1 = 2\cos(\theta) + 1$:

$$P_n(\cos(\theta)) = \cos(n\theta) + \left(\frac{1+\cos(\theta)}{\sin(\theta)}\right)\sin(\theta) = \cos(n\theta) + \frac{\sin(n\theta)}{\tan(\frac{\theta}{2})}$$

$$P_n(\cos(\theta)) = 0 \Leftrightarrow \tan(n\theta) = \tan\left(-\frac{\theta}{2}\right) \Leftrightarrow n\theta = -\frac{\theta}{2} + k\pi \Leftrightarrow \theta = \frac{2k\pi}{2n+1}$$

Les racines de P_n sont donc les $x_{k,n} = \cos\left(\frac{2k\pi}{2n+1}\right)$ pour $1 \leqslant k \leqslant n$.

c) Les nombres $\cos\left(\frac{2\pi}{5}\right)$, $\cos\left(\frac{2\pi}{7}\right)$ et $\cos\left(\frac{2\pi}{9}\right)$ sont respectivement racines de P_2, P_3 et P_4 appartenant à $\mathbb{Q}[X]$, donc ils sont algébriques.

On a vu que P_2 et P_3 n'ont pas de racines rationnelles donc sont irréductible sur $\mathbb{Q}$.

Ainsi ce sont les polynômes minimaux des 2 premiers nombres.

On sait que Q_4 admet ± 1 comme racines donc P_4 $\pm\frac{1}{2}$. On a comme seule racine $-\frac{1}{2}$, on peut donc le factoriser comme suit :

$$P_4(x) = (2x+1)(8x^3 - 6x + 1)$$

$-\frac{1}{2}$ n'est pas racine de $x^3 - \frac{3}{4}x + \frac{1}{8}$ donc c'est le polynôme minimal de $\cos\left(\frac{2\pi}{9}\right)$.

7. a) Le polynôme minimal de α est de degré 3 donc $\dim(\mathbb{Q}[\alpha]) = 3$ et $(1, \alpha, \alpha^2)$ en est une base. En utilisant la formule $\cos(2x) = 2\cos^2(x) - 1$ et le fait que $\alpha^3 = \frac{3}{4}\alpha + \frac{1}{8}$ on trouve $\cos\left(\frac{4\pi}{9}\right) = 2\alpha^2 - 1$ et $\cos\left(\frac{8\pi}{9}\right) = -2\alpha^2 - \alpha + 1$.

b) On a $f(1) = f(1)^2$ donc soit $f(1) = 1$ soit $f(1) = 0$. Par ailleurs on a aussi $f(\alpha^k) = (f(\alpha))^k$ d'où par linéarité $f(\alpha)^3 - \frac{3}{4}f(\alpha) + \frac{1}{8}f(1) = 0$. Si $f(1) = 0$ alors $f(\alpha)(f(\alpha)^2 - \frac{3}{4}) = 0$ et donc $f(\alpha) = 0$ car $\frac{\sqrt{3}}{2} \notin \mathbb{Q}[\alpha]$. Et $f(\alpha^2) = (f(\alpha))^2 = 0$ donc f est l'endomorphisme nul. On écarte ce cas et on choisit donc $f(1) = 1$. Ainsi $f(\alpha)$ est racine de la même équation que α. On a donc les trois possibilités suivantes :

$$f_1(\alpha) = \alpha \quad f_2(\alpha) = \cos\left(\frac{4\pi}{9}\right) = 2\alpha^2 - 1 \quad f_3(\alpha) = \cos\left(\frac{8\pi}{9}\right) = -2\alpha^2 - \alpha + 1$$

On calcule et simplifie les $f_i(\alpha^2) = (f_i(\alpha))^2$ et on obtient les matrices :

$$M_1 = I_3 \quad M_2 = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & -\frac{1}{2} \\ 0 & 2 & -1 \end{pmatrix} \quad M_3 = \begin{pmatrix} 1 & 1 & \frac{1}{2} \\ 0 & -1 & \frac{1}{2} \\ 0 & -2 & 0 \end{pmatrix}$$

Et on vérifie que $M_2M_3 = M_3M_2 = I_3 = M_1$ (le neutre du groupe à trois éléments).

8. a) $S(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. On a donc :

$$|S(r)| = |a_np^n + qa_{n-1}p^{n-1} + \cdots + q^{n-1}a_1p + q^na_0| \times \frac{1}{q^n}$$

Le terme en valeur absolue est non nul (car S irréductible) et entier donc $\geqslant 1$.

On peut donc choisir $C_S = 1$ et pour tout rationnel r, $|S(r)| \geqslant \frac{1}{q^n}$.

b) On utilise la minoration précédente :

$$|S(r)| = |r-\alpha||P(r)| \geqslant \frac{1}{q^n} \Rightarrow |\alpha - r| \geqslant \frac{1}{|P(r)|q^n} \geqslant \frac{K}{q^n}$$

avec K l'inverse du max de $|P(r)|$ sur $[\alpha-1, \alpha+1]$.

c) $\forall k \in \mathbb{N}$, $\frac{1}{10^{k!}} \leqslant \frac{1}{10^k}$ d'où en sommant :

$$t_n \leqslant \frac{1-(\frac{1}{10})^n}{1-\frac{1}{10}} \leqslant \frac{10}{9}$$

Ainsi (t_n) est bornée, et clairement croissante, donc convergente.

$$t - t_n = \sum_{k=n+1}^{+\infty} 10^{-k!} = 10^{-(n+1)!} + 10^{-(n+1)!} \sum_{k=n+1}^{+\infty} 10^{-kk!}$$

Et $\displaystyle\sum_{k=n+1}^{+\infty} 10^{-kk!} < \sum_{k=n+1}^{+\infty} (\frac{1}{10})^k = \frac{10}{9}(1-(1-(\frac{1}{10})^{n+1})) = \frac{10}{9}(\frac{1}{10})^{n+1} < 1.$

Par conséquent $|t - t_n| \leqslant 2 \times 10^{-(n+1)!}$.

Supposons t algébrique et prenons $r = t_k$ donc $q = 10^{k!}$, il vient :

$$|t - t_k| \geqslant \frac{K}{10^{nk!}}$$

Mais via l'inégalité précédente on tire :

$$K \leqslant 2 \times 10^{-k!(k+1-n)} \to 0 \text{ quand } k \to +\infty$$

On aurait alors $K \leqslant 0$, absurde puisque $K > 0$. Donc t est transcendant.

Seconde partie

1. • Soit $A_1(x_1, y_1)$ et $A_2(x_2, y_2)$ dans $\mathcal{K}$. La droite les joignants : $y = ax + b$.

$y_1 = ax_1 + b$, $y_2 = ax_2 + b$, et par soustraction

$$y_1 - y_2 = a(x_1 - x_2) \Rightarrow a = (y_1 - y_2)(x_1 - x_2)^{-1} \in K,\ b = y_1 - ax_1 \in K$$

Pour le cercle centré en A de rayon AB : $(x-x_1)^2 + (y-y_1)^2 = d^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2$.

• Intersection $a_1x + b_1 = a_2x + b_2 \Rightarrow x = (b_2 - b_1)(a_1 - a_2)^{-1} \in K$.

• $(x-x_1)^2 + (a_1x + b - y_1)^2 = d^2 \Rightarrow$ équation du second degré en x. Si $\sqrt{\Delta} \in K$ alors c'est un point de $\mathcal{K}$ sinon les coordonnées de ce point sont dans $K[\sqrt{\Delta}]$ extension quadratique de K.

• Même chose pour le cercle.

2. a) On trace les cercles $\mathcal{C}(A, BC)$ et $\mathcal{C}(C, AB)$, D est à une des intersections.

Pour tracer la parallèle à Δ passant par A on choisit 2 points B et C de Δ et on construit le point D comme ci-dessus. La droite recherchée passe par les points A et D.

b) • $J = \mathcal{C}(O, OI = 1) \cap \mathcal{D}(O, I)$. Pour K on construit au préalable les points A et B intersections de $\mathcal{C}(J, JI)$ et $\mathcal{C}(I, JI)$. K est l'intersection de la droite (AB) et du cercle unité (d'ordonnée positive).

• Par abus je confondrai le point $A(\alpha, 0)$ avec son abscisse. Supposons $\alpha > \beta$ alors $\alpha + \beta$ s'obtient en intersectant le cercle $\mathcal{C}(\alpha, \beta)$ avec l'axe (O_x).

On place maintenant β sur (O_y). On trace la droite $(\beta\alpha)$ et la droite qui lui est parallèle passant par K, elle coupe (O_x) en z. Par le théorème de Thalès il vient $\frac{z}{\alpha} = \frac{1}{\beta} \Rightarrow z = \frac{\alpha}{\beta}$.

On construit à partir de ce qui précède $\gamma = \frac{1}{\beta}$ puis $\frac{\alpha}{\gamma} = \alpha\beta$.

• On trace comme suggéré le cercle $\mathcal{C}$ de diamètre $J\alpha$. On sait construire $\alpha - 1$, on appelle T l'intersection de $\mathcal{C}$ et du cercle de centre J et de rayon $\alpha - 1$. Le triangle JTA est inscrit dans un demi-cercle donc est rectangle. D'après le théorème de Pythagore on a donc $AT^2 = JA^2 - JT^2 = (\alpha+1)^2 - (\alpha-1)^2 = 4\alpha$ d'où $AT = 2\sqrt{\alpha}$ que l'on sait déterminer le milieu. Donc $\sqrt{\alpha}$ est constructible.

3. a) M construit à partir de $O, I, M_1, ..., M_{n-1}$. M_1 construit à partir de O et I via les 4 opérations élémentaires sur $\mathbb{Q} = K_0$. Si M_2 est construit aussi via la combinaison de ces 4 opérations à partir de O, I et M_1, ses coordonnées restent dans le corps K_0. Mais si maintenant la construction de M_2 fait intervenir une racine $\sqrt{\alpha}$ où $\alpha \neq k^2$ est dans K_0, alors les coordonnées de M_2 sont dans l'extension quadratique $K_0[\sqrt{\alpha}] = K_1$, et ainsi de suite jusqu'à l'obtention du point M.

b) Initialisation : $(a, b) \in K_0^2$, $M(a, b)$ constructible car a et b le sont via l'opération $\frac{\alpha}{\beta}$.

Hérédité : $(x_p, y_p) \in K_n$, les points $M(x_p, y_p)$ sont constructibles par hypothèses.

$$K_{n+1} = K_n[\sqrt{\alpha}] = \left\{ x = \sum_{p=0}^{q} x_p (\sqrt{\alpha})^p \right\}$$

Comme $\sqrt{\alpha}$ et les x_p sont constructibles, par produits et sommes, les $x \in K_{n+1}$ sont constructibles. Ce qui achève la récurrence.

4. a) Dans G vu comme F-ev, tout élément s'écrit $x = f_1 g_1 + \cdots + f_q g_q$. H comme $G - ev$:

$x = \lambda_1 h_1 + \cdots + \lambda_r h_r = (f_{1,1} g_1 + \cdots + f_{1,q} g_q) h_1 + (f_{2,1} g_1 + \cdots + f_{2,q} g_q) h_2 + \cdots + (f_{r,1} g_1 + \cdots + f_{r,q} g_q) h_r$

Les $h_i g_j$ forment une base de H vu comme F-ev, qui sont au nombre de rq.

$$\dim_F(H) = rq$$

b) D'après la question précédente, en itérant il vient $\dim_{\mathbb{Q}}(K_n) = 2^n$.

c) Si α est constructible il appartient à un certain K_n. $\mathbb{Q}[\alpha]$ est le plus petit corps contenant $\mathbb{Q}$ et α donc :

$$\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset K_n$$

Toujours d'après a) on a

$$\dim_{\mathbb{Q}}(K_n) = \dim_{\mathbb{Q}[\alpha]}(K_n) \times \dim_{\mathbb{Q}}(\mathbb{Q}[\alpha])$$

On a $\dim_{\mathbb{Q}}(K_n) = 2^n$ et $\dim_{\mathbb{Q}}(\mathbb{Q}[\alpha]) = d(\alpha, \mathbb{Q})$ est donc une puissance de 2.

Pour la racine cubique de 2, son polynôme minimal est $X^3 - 2$ qui est de degré 3, donc non constructible.

5. Si $\cos\left(\frac{2\pi}{n}\right)$ est constructible alors les $\cos\left(\frac{2k\pi}{n}\right)$ aussi par les formules de trigo.

$n = 3$: oui car $\cos\left(\frac{2\pi}{3}\right) = -\frac{1}{2}$.
$n = 4$: oui car $\cos\left(\frac{2\pi}{4}\right) = 0$.
$n = 5$: oui car polynôme minimal P_2 de degré 2.
$n = 6$: oui car $\cos\left(\frac{\pi}{3}\right) = \frac{1}{2}$.
$n = 7$: non car polynôme minimal P_3 de degré 3.
$n = 8$: oui car $\cos\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2}$.
$n = 9$: non car polynôme minimal de degré 3.
$n = 10$: oui car $\cos\left(\frac{\pi}{5}\right) = \frac{\cos\left(\frac{2\pi}{5}\right)-1}{2}$.

Les polynômes réguliers à 7 et 9 côtés ne sont donc pas constructibles.